Consiglio dell'Unione europea

Bruxelles, 16 gennaio 2025
(OR. en)

5426/25

CYBER 21
SAN 15

NOTA DI TRASMISSIONE

Origine:	Segretaria generale della Commissione europea, firmato da Martine DEPREZ, direttrice
Data:	15 gennaio 2025
Destinatario:	Thérèse BLANCHET, segretaria generale del Consiglio dell'Unione europea
n. doc. Comm.:	COM(2025) 10 final
Oggetto:	COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI Piano d'azione europeo sulla cibersicurezza degli ospedali e dei prestatori di assistenza sanitaria

Si trasmette in allegato, per le delegazioni, il documento COM(2025) 10 final.

All.: COM(2025) 10 final

COMMISSIONE
EUROPEA

Bruxelles, 15.1.2025
COM(2025) 10 final

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI

Piano d'azione europeo sulla cibersicurezza degli ospedali e dei prestatori di assistenza sanitaria

1. Introduzione

Il contesto di sicurezza dell'UE sta cambiando rapidamente: stiamo assistendo a un'escalation di attacchi ibridi e di attacchi informatici che mirano a destabilizzare la nostra società, cercando di creare divisioni e perturbazioni, ma anche profitti attraverso attività informatiche criminali. L'Europa deve pertanto rafforzare urgentemente la propria preparazione e la propria resilienza a fronte di questa nuova realtà, in tutti i settori e in linea con un approccio esteso a tutta la società e a tutta l'amministrazione, come invocato nella relazione del consigliere speciale della presidente della Commissione europea Sauli Niinistö.

Sistemi sanitari sicuri e resilienti sono una pietra angolare del modello sociale dell'UE. Gli ospedali e i sistemi sanitari si trovano tuttavia ad affrontare minacce crescenti, provenienti in particolare da bande criminali che si servono dei ransomware e li prendono di mira a fini di lucro, attratte dall'elevato valore dei dati dei pazienti, comprese le cartelle cliniche elettroniche. Negli ultimi quattro anni il settore sanitario è infatti diventato quello più colpito, anche durante la pandemia di COVID-19, quando le infrastrutture sanitarie sono state oggetto di un numero sempre maggiore di attacchi informatici. Gli attacchi informatici contro ospedali e prestatori di assistenza sanitaria stanno causando danni diretti alle persone, ritardando le procedure mediche, paralizzando i reparti di pronto soccorso e potrebbero, in casi estremi, causare la perdita di vite umane.

La posta in gioco è ancora più elevata in quanto nel settore è in atto una trasformazione digitale di vitale importanza. La sanità digitale e l'utilizzo e il riutilizzo dei dati sanitari possono rendere possibili modelli di assistenza più adatti alle esigenze e alle preferenze delle persone e dei pazienti, prevenendo l'insorgenza di una malattia o consentendo trattamenti più precoci. L'integrazione di strumenti e soluzioni digitali nei processi clinici, così come l'utilizzo e il riutilizzo dei dati sanitari possono orientare decisioni cliniche migliori, contribuire all'automazione in campo sanitario e a un'assistenza più rapida e di migliore qualità per i pazienti. Anche gli strumenti digitali, l'utilizzo dei dati e i dispositivi medici, che sono spesso connessi a internet e sfruttano l'intelligenza artificiale (IA), sono fondamentali per affrontare sfide quali la carenza di operatori sanitari.

Allo stesso tempo, con gli strumenti digitali aumentano altresì i potenziali obiettivi dei criminali informatici. Inoltre alcuni attori statali non risparmiano le strutture sanitarie nei loro attacchi, come dimostrato dall'attuale guerra di aggressione della Russia nei confronti dell'Ucraina. Il settore diviene pertanto un bersaglio potenziale di attacchi informatici nel quadro di una più ampia campagna ibrida. Gli attacchi informatici non si limitano a mettere a repentaglio la sicurezza dei pazienti, ma erodono anche la fiducia dei cittadini nelle infrastrutture sanitarie e comportano costi notevoli per la ripresa. Oltre a proteggere dagli attacchi informatici, un'infrastruttura digitale resiliente e sicura è essenziale anche ai fini del sostegno all'attuazione e alla piena realizzazione dello spazio europeo dei dati sanitari[1] (*European Health Data Space*, EHDS).

È pertanto giunto il momento di migliorare e rafforzare la cibersicurezza e la resilienza degli ospedali e dei prestatori di assistenza sanitaria europei, come sottolineato dalla presidente von der Leyen nei suoi orientamenti politici per la Commissione 2024-2029[2]. Il piano d'azione risponde all'urgenza della

[1] https://www.consilium.europa.eu/it/press/press-releases/2024/03/15/european-health-data-space-council-and-parliament-strike-provisional-deal/

[2] https://commission.europa.eu/document/e6cd4328-673c-4e7a-8683-f63ffb2cf648_it.

situazione e alle minacce specifiche a cui è esposto il settore. Per quanto non esista una soluzione semplice e miracolosa alle sfide in materia di cibersicurezza nell'assistenza sanitaria, il piano d'azione invoca un rafforzamento della prevenzione e della preparazione e un miglior coordinamento dell'approccio alla solidarietà, sfruttando le competenze del settore europeo della cibersicurezza. Il piano d'azione riflette pertanto l'approccio dell'UE in materia di sicurezza che sarà ulteriormente sviluppato e formalizzato nella prossima strategia europea di sicurezza interna, definendo una risposta globale volta ad affrontare tutte le minacce alla sicurezza interna e concentrandosi sulla capacità di anticipare le minacce, prevenire i danni e proteggere le persone, agendo a tutti i livelli con un approccio esteso a tutta la società.

Il settore sanitario comprende un ampio numero di entità e attori, tra cui ospedali, cliniche, case di cura, centri di riabilitazione e vari prestatori di assistenza sanitaria, oltre all'industria farmaceutica, medica e biotecnologica, ai fabbricanti di dispositivi medici e agli istituti di ricerca sanitaria. Il piano d'azione si concentra principalmente sulla cibersicurezza degli ospedali e dei prestatori di assistenza sanitaria, intesi come una qualsiasi persona fisica o giuridica o qualsiasi altra entità che presti legalmente assistenza sanitaria nel territorio di uno Stato membro[3]. Gli ospedali e i prestatori di assistenza sanitaria sono interdipendenti con altri enti sanitari e sono i più vicini alle persone. Allo stesso tempo, le misure volte a rafforzare la cibersicurezza degli ospedali e dei prestatori di assistenza sanitaria dovrebbero anche affrontare i rischi che interessano la catena di approvvigionamento e l'ecosistema a livello più ampio, derivanti ad esempio da soggetti che utilizzano dati sanitari per la ricerca e l'apprendimento automatico o che producono dispositivi medici, in particolare dispositivi medici basati sul digitale che si collegano a internet o ad altri dispositivi ("internet delle cose").

Per quanto la sicurezza dei sistemi sanitari sia in primo luogo di competenza nazionale, la sanità è anche un settore critico a norma della direttiva relativa a misure per un livello comune elevato di cibersicurezza nell'UE (NIS 2)[4]. I criminali informatici e altri autori delle minacce operano a livello transfrontaliero e anche le sfide in materia di cibersicurezza cui devono far fronte le organizzazioni sanitarie sono simili in tutti gli Stati membri. La cooperazione a livello europeo è preziosa ai fini della condivisione e del potenziamento delle migliori pratiche a livello di UE e nazionale. Il piano d'azione propone pertanto un coordinamento e misure a livello di UE, invitando nel contempo gli Stati membri ad agire e a fare la differenza per l'assistenza sanitaria e per il più ampio ecosistema sanitario.

Il piano d'azione è incentrato sulla creazione di capacità nel settore, in primo luogo per la **prevenzione** degli incidenti di cibersicurezza, in quanto prevenire è sempre meglio che curare. In secondo luogo esso illustra le azioni volte a migliorare la condivisione delle informazioni in materia di cibersicurezza e la capacità di **rilevare** le minacce informatiche, consentendo una reazione più rapida. In terzo luogo il piano d'azione prevede misure per una migliore **risposta** agli incidenti e per la successiva **ripresa** e infine

[3] Articolo 3, lettera g), della direttiva 2011/24/UE del Parlamento europeo e del Consiglio, del 9 marzo 2011, concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=celex:32011L0024.

[4] Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (direttiva NIS 2) (https://eur-lex.europa.eu/eli/dir/2022/2555).

prevede modalità atte a **dissuadere** gli autori di minacce informatiche dal lanciare attacchi contro i sistemi sanitari in Europa.

Il piano d'azione sarà attuato di concerto con i prestatori di assistenza sanitaria e con l'ecosistema sanitario a livello più ampio, con gli Stati membri e con la comunità della cibersicurezza. Un approccio collaborativo è fondamentale per definire e perfezionare ulteriormente le azioni più incisive, affinché tutti i prestatori critici di assistenza sanitaria in Europa possano trarne vantaggio. La presente comunicazione sarà pertanto accompagnata dall'avvio di una consultazione globale dei portatori di interessi, dell'industria e degli Stati membri. La cooperazione internazionale è importante per la cibersicurezza, data la natura interconnessa e senza frontiere delle minacce informatiche. Minacce alla cibersicurezza analoghe sono presenti anche nei paesi dell'allargamento e del vicinato e in altri paesi che sono partner strategici dell'UE, e ciò può mettere a repentaglio la sicurezza delle infrastrutture critiche nell'UE. Sarà pertanto importante riflettere sugli insegnamenti tratti dall'attuazione del piano d'azione anche nella cooperazione dell'UE sia con i paesi dell'allargamento sia con altri paesi partner, alla luce dei livelli di minaccia ai quali tali paesi sono rispettivamente esposti.

2. La sfida della cibersicurezza degli ospedali e dei prestatori di assistenza sanitaria

Minacce informatiche al settore sanitario

Gli attacchi informatici sono in aumento a livello mondiale e all'interno dell'UE e il panorama delle minacce è sempre più complesso e dinamico. L'evoluzione dell'IA sta dotando i criminali e i malintenzionati di strumenti potenti per aumentare la precisione e l'impatto delle loro operazioni, ma ridefinisce nel contempo le possibilità di ciberdifesa rendendo possibile un'azione automatizzata e in tempo reale contro gli attacchi.

I ransomware continuano a rappresentare una sfida critica per la cibersicurezza nell'UE e a livello mondiale e una relazione ne stima il costo annuo globale a oltre 250 miliardi di EUR entro il 2031[5]. Quando colpiscono, gli autori di attacchi ransomware non si limitano a criptare i dati delle vittime per chiedere un riscatto, ma rendono pubblico un numero gradualmente crescente di informazioni sensibili per esercitare ulteriore pressione. Un'altra sfida di rilievo è rappresentata dalle vulnerabilità di software e hardware: secondo l'Agenzia dell'Unione europea per la cibersicurezza (ENISA)[6], l'assistenza sanitaria è il settore che ha dichiarato il maggior numero di incidenti di sicurezza connessi a tali vulnerabilità[7]. Altre minacce crescenti comprendono gli attacchi distribuiti di negazione del servizio (*distributed*

[5] Cybersecurity Ventures (1° giugno 2024): *Global Ransomware Damage Costs Predicted to Exceed $265 Billion by 2031*. Disponibile all'indirizzo https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.
[6] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione ("regolamento sulla cibersicurezza") (https://eur-lex.europa.eu/eli/reg/2019/881/oj/ita).
[7] Relazione dell'ENISA sul panorama delle minacce: settore sanitario (luglio 2023).

denial-of-service, DDoS), concepiti per sovraccaricare il sistema preso di mira con una enorme quantità di traffico che lo rende inaccessibile agli utenti legittimi[8].

Il settore sanitario si trova ad affrontare tendenze analoghe per quanto riguarda le minacce alla cibersicurezza, con una forte enfasi sugli attacchi ransomware. Secondo l'ENISA, nel periodo 2021-2023 i ransomware hanno rappresentato il 54 % degli incidenti di cibersicurezza analizzati nel settore sanitario. L'83 % degli attacchi aveva motivazione finanziaria, dato l'elevato valore dei dati sanitari, mentre il 10 % degli attacchi nasceva da motivazioni ideologiche[9]. Analogamente, da una relazione della Commissione del 2024 emerge che il 71 % degli attacchi che hanno avuto conseguenze sull'assistenza ai pazienti, quali ritardi nelle cure o nella diagnosi e difficoltà di accesso ai servizi di emergenza, erano del tipo ransomware[10]. Gli attacchi ransomware possono avere conseguenze particolarmente negative sulla prestazione di servizi sanitari, mettendo a rischio la sicurezza dei pazienti, e sono inoltre spesso associati a violazioni dei dati dei pazienti[11], che comprendono sovente dati sensibili relativi alla salute, e del diritto fondamentale delle persone alla protezione dei dati personali.

Allo stesso tempo la crescente digitalizzazione dell'assistenza sanitaria comporta un ampliamento della superficie di attacco. Secondo la relazione sullo stato del decennio digitale 2024, in media il 79 % dei cittadini dell'UE ha accesso online alle proprie cartelle cliniche elettroniche nell'assistenza sanitaria di base[12]. Le cartelle cliniche elettroniche, i sistemi di informazione clinica, i sistemi di flusso di lavoro ospedaliero, i sistemi informatici per la gestione del rimborso delle cure, i sistemi di diagnostica per immagini e i dispositivi medici utilizzati a fini diagnostici o di monitoraggio dei pazienti sono tutti esempi di strumenti digitali che possono avere un ruolo importante nel potenziare l'efficienza e le prestazioni del settore sanitario, ma sono anche obiettivi potenziali di un attacco alla cibersicurezza. Attività specifiche di assistenza sanitaria, come la terapia intensiva e la radiologia per immagini, o settori medici come l'oncologia e la cardiologia, che dipendono fortemente da dispositivi basati sul digitale, sono particolarmente a rischio di attacchi informatici. Inoltre i problemi legati alla catena di approvvigionamento possono portare all'acquisto di dispositivi privi di una sicurezza informatica sufficiente, aggravando i rischi generali esistenti.

Durante la pandemia di COVID-19, ad esempio, un attacco ransomware ha paralizzato ampie parti del sistema sanitario irlandese, causando in 31 dei 54 ospedali che offrono servizi quali pronto soccorso e terapia intensiva la cancellazione di almeno alcuni servizi la mattina dell'incidente[13]. I servizi sanitari

[8] Relazione dell'ENISA sul panorama delle minacce 2024.
[9] Relazione dell'ENISA sul panorama delle minacce: settore sanitario (luglio 2023). Nella relazione sono presi in esame i prestatori di assistenza sanitaria e altri tipi di organizzazioni, comprese le organizzazioni che svolgono attività di ricerca in campo sanitario, i soggetti che fabbricano determinati prodotti sanitari, le autorità sanitarie, le assicurazioni sanitarie, le strutture di trattamento residenziale e i prestatori di servizi sociali. Disponibile all'indirizzo https://www.enisa.europa.eu/publications/health-threat-landscape.
[10] Commissione europea, Centro comune di ricerca, Reina, V. e Griesinger, C., *Cyber security in the health and medicine sector — A study on available evidence of patient health consequences from cyber accidents in healthcare settings*, Ufficio delle pubblicazioni dell'Unione europea, 2024, https://data.europa.eu/doi/10.2760/693487.
[11] Secondo la relazione dell'ENISA sul panorama delle minacce per il settore sanitario, la violazione o il furto di dati sono stati confermati nel 43 % degli incidenti di ransomware analizzati.
[12] Relazione sullo stato del decennio digitale 2024.
[13] Irish Health Service Executive (2021): *Conti cyber attack on the HSE: Independent Post Incident Review*.

hanno dovuto tornare ai registri cartacei, rallentando l'efficienza delle operazioni. L'attacco proveniva da un'e-mail di phishing contenente un allegato dannoso[14]. L'incidente ha dimostrato il potenziale degli attacchi informatici che si diffondono in diversi sistemi e, di conseguenza, l'importanza di proteggere l'intera superficie di attacco di un'organizzazione sanitaria, sottolineando inoltre l'importanza di garantire l'igiene informatica e la cultura della cibersicurezza di base in tutte le organizzazioni.

Maturità della cibersicurezza degli ospedali e dei prestatori di assistenza sanitaria

Il panorama sanitario dell'UE è molto eterogeneo: gli ospedali e gli altri prestatori di assistenza sanitaria presentano differenze significative in termini di proprietà, struttura e dimensioni nei vari Stati membri. La governance dell'assistenza sanitaria può essere basata su un approccio centralizzato in alcuni casi a livello nazionale, in altri a livello regionale e locale; la proprietà dei prestatori di assistenza sanitaria può essere pubblica o privata. Possono inoltre sussistere differenze anche all'interno dello stesso paese, ad esempio quando vi sono notevoli disparità socioeconomiche e territoriali tra le regioni, che danno vita a un quadro complesso. Questo panorama sanitario complesso può essere messo a dura prova da importanti crisi sanitarie dovute a malattie trasmissibili, come la pandemia di COVID-19, ma anche ad altri rischi sanitari, connessi ad esempio ai cambiamenti climatici. Infine, il livello di digitalizzazione e adozione della tecnologia da parte dei prestatori di assistenza sanitaria risulta notevolmente variabile e frammentato. Il fatto che l'indisponibilità del servizio causata da un incidente di cibersicurezza possa causare gravi danni e pregiudizi ai pazienti anche in strutture sanitarie di piccole dimensioni, comprese cliniche o servizi medici di emergenza che forniscono un servizio essenziale a un numero relativamente basso di utenti, è un esempio della complessità sopra descritta.

Secondo la relazione dell'ENISA del 2024 sullo stato della cibersicurezza nell'Unione[15], la maturità del settore sanitario dell'UE è moderata e sussistono ampie differenze nel livello di maturità della cibersicurezza tra gli enti sanitari in Europa. Sono emerse carenze in alcuni aspetti fondamentali, quali risorse umane sufficienti, conoscenza da parte delle organizzazioni delle loro catene di approvvigionamento delle tecnologie dell'informazione e della comunicazione (TIC) e installazione di elementi di sicurezza aggiornati nei prodotti. Il settore incontra difficoltà per quanto riguarda l'igiene informatica di base e le misure fondamentali di sicurezza, come dimostra il fatto che per quasi tutte le organizzazioni sanitarie prese in esame la realizzazione di valutazioni dei rischi di cibersicurezza rappresenta una sfida; pressoché la metà di tali organizzazioni non ha peraltro mai effettuato un'analisi dei rischi[16].

Un'altra sfida significativa per la cibersicurezza degli ospedali è l'intersezione tra tecnologia dell'informazione (IT) e tecnologia operativa (OT), dove si incontrano diverse priorità in materia di sicurezza per quanto riguarda la riservatezza, la disponibilità e l'affidabilità; una violazione commessa in un settore in corrispondenza di detta intersezione può colpire anche l'altro settore. Nella relazione

[14] Irish Health Service Executive: *Cyber-attack and HSE response*. Disponibile all'indirizzo https://www2.hse.ie/services/cyber-attack/what-happened/.

[15] ENISA: *2024 Report on the State of Cybersecurity in the Union* (settembre 2024). Disponibile all'indirizzo https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

[16] Relazione dell'ENISA sul panorama delle minacce: settore sanitario (luglio 2023). Disponibile all'indirizzo https://www.enisa.europa.eu/publications/health-threat-landscape.

dell'ENISA del 2024 sullo stato della cibersicurezza nell'Unione si sottolinea inoltre che il settore sanitario non riesce a garantire in maniera adeguata la sicurezza dei prodotti e dei processi TIC che utilizza, a causa della grande varietà di entità, dispositivi e prodotti sanitari.

Detta varietà, associata a livelli variabili di consapevolezza informatica tra il personale ospedaliero e la dirigenza, rende il compito di garantire la cibersicurezza dei sistemi sanitari una sfida complessa. Secondo l'Eurobarometro del 2024 sulle competenze informatiche, ad esempio, solo il 25 % delle imprese oggetto dell'indagine nel settore della sanità, dell'istruzione e dell'assistenza sociale aveva fornito formazione o svolto attività di sensibilizzazione in materia di cibersicurezza nei 12 mesi precedenti[17]. È necessario intervenire per promuovere una cultura della consapevolezza in materia di cibersicurezza tra gli operatori sanitari in prima linea. Le rotazioni del personale, l'uso di postazioni di lavoro condivise, la cattiva gestione dell'autenticazione e l'uso di media rimovibili sono, ad esempio, ulteriori fonti di vulnerabilità che incidono sulla cibersicurezza dei prestatori di assistenza sanitaria[18].

In molti casi, IT e OT sono almeno in parte esternalizzate. Dall'Eurobarometro del 2024 è emerso che nei settori della sanità, dell'istruzione e dell'assistenza sociale si registra la percentuale più elevata di imprese che esternalizzano almeno alcuni aspetti della loro cibersicurezza, pari al 57 % delle imprese oggetto dell'indagine[19]. Vi è analogamente una forte tendenza a migrare verso il cloud computing, determinata dalla necessità di rendere scalabile l'archiviazione e la gestione dei dati, di conseguire l'efficienza in termini di costi, di migliorare la collaborazione e di supportare tecnologie avanzate come l'IA e l'internet delle cose mediche. Nel 2022 il 58 % delle organizzazioni sanitarie ha utilizzato una piattaforma sanitaria digitale basata sul cloud[20]. Tale cambiamento tuttavia, pur essendo in grado di apportare efficienze significative, comporta anche rischi che richiedono decisioni informate in materia di appalti e configurazione sicura.

La creazione di capacità e i finanziamenti sono aspetti generali che riguardano tutte le sfide descritte finora. I finanziamenti per la cibersicurezza nel settore sanitario sono stati limitati e rappresentano tuttora una sfida universale in tutta l'UE[21]. Inoltre le sfide relative ai finanziamenti emergono in un contesto caratterizzato dall'invecchiamento della popolazione, che nei prossimi decenni dovrebbe creare pressioni di bilancio diffuse sui sistemi sanitari europei.

L'uso continuo di strumenti obsoleti e di sistemi preesistenti, le risorse limitate per prevenire gli incidenti o reagirvi e le lacune in termini di maturità della cibersicurezza derivano spesso da carenze di finanziamento. Il conseguimento di un equilibrio tra un'infrastruttura sicura e digitale aggiornata e gli

[17] Eurobarometro Flash 547 sulle competenze informatiche (maggio 2024). Disponibile all'indirizzo https://europa.eu/eurobarometer/surveys/detail/3176.
[18] Panacea – People-centric cybersecurity in healthcare (2021), *White Paper – Lessons learnt from PANACEA on the cyber-protection of hospitals and care centres*.
[19] Eurobarometro Flash 547 sulle competenze informatiche (maggio 2024). Disponibile all'indirizzo https://europa.eu/eurobarometer/surveys/detail/3176.
[20] ENISA: *NIS Investments*, relazione del 2022 (novembre 2022). Disponibile all'indirizzo https://www.enisa.europa.eu/publications/nis-investments-2022.
[21] L'organizzazione e la fornitura di servizi sanitari e di assistenza medica sono di competenza nazionale a norma dell'articolo 168 del trattato sul funzionamento dell'Unione europea e il finanziamento dei sistemi sanitari varia da uno Stato membro all'altro.

altri investimenti necessari per migliorare l'assistenza ai pazienti, come l'assunzione di medici e altri operatori sanitari, l'attuazione di nuovi metodi diagnostici e terapeutici e l'acquisizione di dispositivi, costituisce per gli ospedali una sfida costante. Secondo l'ENISA[22] il settore sanitario occupa solo il 7° posto tra i 12 settori esaminati per quanto riguarda la percentuale della spesa per la sicurezza delle informazioni sul totale della spesa informatica: la media nel settore sanitario è pari all'8,3 %.

3. Centro europeo di sostegno alla cibersicurezza per ospedali e prestatori di assistenza sanitaria

Il quadro dell'UE in materia di cibersicurezza offre un'ampia gamma di strumenti che dovrebbero essere sfruttati per migliorare la sicurezza e la resilienza degli ospedali e dei prestatori di assistenza sanitaria. Per far fronte alle numerose sfide sopra evidenziate, è necessario sviluppare un approccio strategico unificato a livello di UE, che riunisca le risorse, le competenze e gli strumenti necessari per affrontare efficacemente le minacce informatiche. Una panoramica completa e una pianificazione e un coordinamento migliori sono essenziali per aiutare i prestatori di assistenza sanitaria in tutta l'UE a rafforzare le loro difese. L'ENISA si trova a tal fine nella posizione migliore per istituire, all'interno della sua organizzazione, un apposito **centro europeo di sostegno alla cibersicurezza per ospedali e prestatori di assistenza sanitaria**[23] nell'ambito del suo mandato[24] di salvaguardare e sostenere le infrastrutture critiche dell'UE.

Il centro di sostegno dovrebbe progressivamente **sviluppare un catalogo completo dei servizi che risponda alle esigenze degli ospedali e dei prestatori di assistenza sanitaria**, delineando la gamma di servizi disponibili a fini di preparazione, prevenzione, rilevamento e risposta. In collaborazione con le autorità degli Stati membri e attingendo alle esperienze degli ospedali e dei prestatori di assistenza sanitaria, il centro di sostegno dovrebbe sviluppare un archivio di facile accesso e di facile utilizzo di tutti gli strumenti disponibili a livello europeo, nazionale e regionale. Nello svolgimento delle sue attività il centro dovrebbe garantire un coordinamento adeguato con gli Stati membri e contribuire alla definizione delle priorità riguardo alle azioni e alla loro realizzazione, secondo necessità, in tempo reale.

Quale importante elemento costitutivo per lo sviluppo del catalogo dei servizi del centro di sostegno, la Commissione proporrà di avviare progetti pilota in tutta l'UE per elaborare le migliori pratiche di igiene informatica e di valutazione dei rischi di sicurezza, come pure per far fronte alla necessità di un monitoraggio continuo della cibersicurezza, di intelligence sulle minacce e di una risposta agli incidenti che si avvalga di soluzioni di cibersicurezza all'avanguardia. I risultati di tali progetti pilota, che saranno finanziati dal programma Europa digitale e realizzati dal Centro europeo di competenza per la

[22] ENISA: *NIS Investments*, relazione del 2022 (novembre 2022). Disponibile all'indirizzo https://www.enisa.europa.eu/publications/nis-investments-2022.

[23] Nel presente documento, "centro di sostegno" è utilizzato in modo intercambiabile.

[24] Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 ("regolamento sulla cibersicurezza") (GU L 151 del 7.6.2019, pag. 15).

cibersicurezza (*European Cybersecurity Competence Centre*, ECCC), orienteranno azioni ulteriori a livello di UE, compreso il lavoro del centro di sostegno.

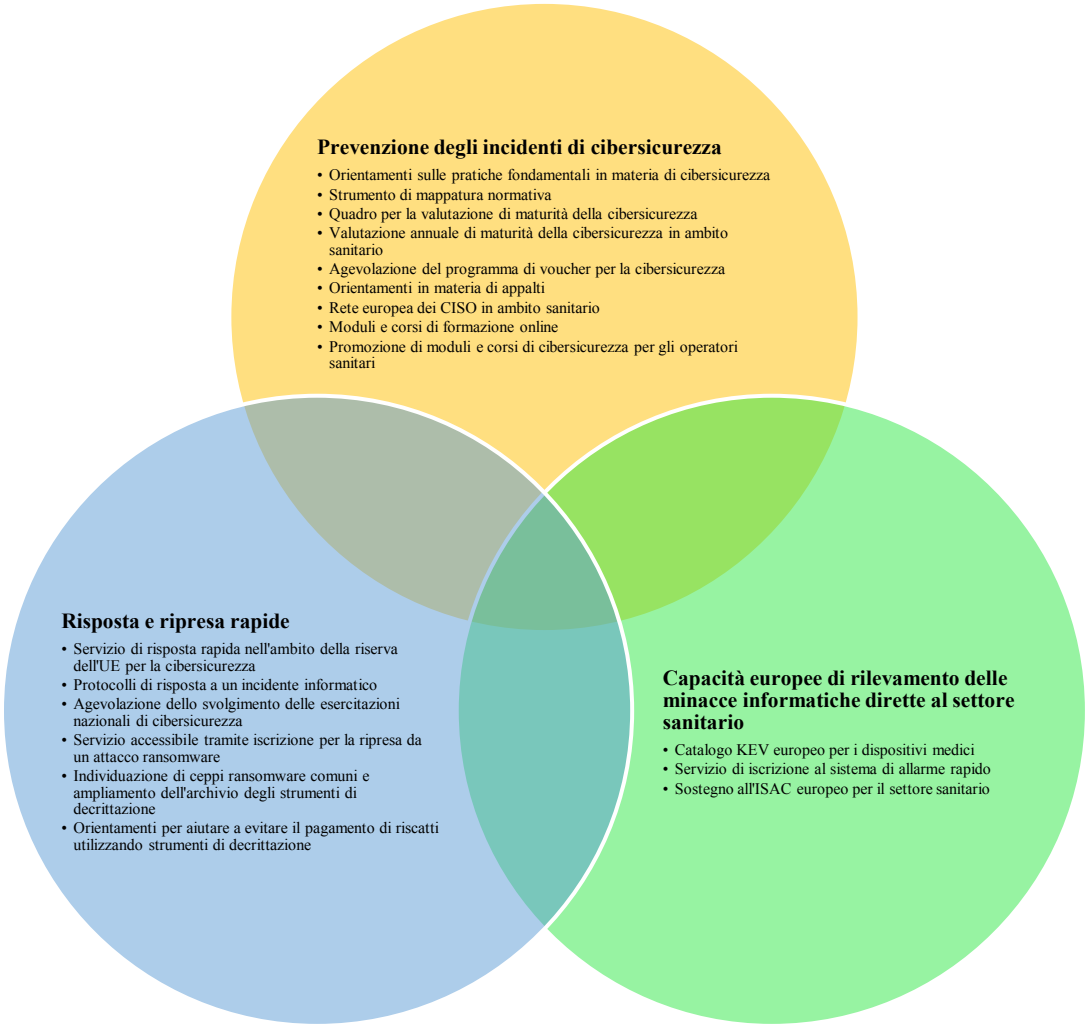

Figura 1: concetti per il catalogo dei servizi del centro di sostegno per ospedali e prestatori di assistenza sanitaria

3.1. Prevenzione degli incidenti di cibersicurezza

Azioni semplici per migliorare la situazione

Secondo una stima le misure di cibersicurezza di base, quali l'aggiornamento costante dei sistemi, la gestione dei backup e l'implementazione dell'autenticazione a più fattori, possono proteggere le

organizzazioni dal 98 % degli attacchi[25]. Molte delle misure più incisive in materia di igiene informatica e gestione dei rischi sono relativamente semplici da adottare e sono pertanto un obiettivo di facile conseguimento per migliorare la cibersicurezza. Uno dei ruoli chiave del centro di sostegno dovrebbe pertanto essere **l'elaborazione di orientamenti chiari e mirati che diano risalto alle pratiche fondamentali in materia di cibersicurezza e aiutino i prestatori di assistenza sanitaria ad attuarle**. Tale sostegno non deve limitarsi ai grandi ospedali, ma prevedere anche consulenze personalizzate per gli enti di dimensioni inferiori, come gli ambulatori locali dei medici generalisti e le cliniche specializzate, che spesso non dispongono delle risorse per costituire appositi team che si occupino di cibersicurezza, ma sono altrettanto vulnerabili agli attacchi. È inoltre necessario tenere conto dell'importanza regionale di enti sanitari specifici per garantire l'assistenza ai pazienti, ad esempio nelle zone scarsamente popolate. Anche gli istituti di ricerca sanitaria che gestiscono grandi quantità di dati personali sensibili potrebbero beneficiare di orientamenti sulle misure di base in materia di cibersicurezza per rafforzare la loro resilienza.

Le organizzazioni sanitarie sono altresì soggette a una serie di obblighi in materia di cibersicurezza derivanti dalla legislazione dell'UE[26]. Sebbene gli obblighi siano fondamentali per garantire una base comune di livello elevato per la cibersicurezza e la sicurezza dei dati, è essenziale garantire che il panorama normativo non risulti inutilmente complicato oneroso. Un'estrema attenzione alla conformità non dovrebbe pregiudicare l'obiettivo di promuovere una forte cultura della cibersicurezza. Uno **strumento di mappatura normativa di facile accesso può contribuire a ridurre al minimo gli oneri amministrativi per gli enti soggetti a molteplici strumenti normativi**. Oltre a elaborare orientamenti e strumenti, il centro di sostegno dovrebbe collaborare a stretto contatto con la Commissione e con gli Stati membri per sviluppare e diffondere quanto prima il suddetto strumento. Il centro di sostegno svolgerebbe pertanto un ruolo importante nel rendere semplice la comprensione e l'attuazione della

[25] *Microsoft Digital Defense Report 2022*. Disponibile all'indirizzo https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2022.

[26] Come la direttiva NIS2; regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali (regolamento sulla ciberresilienza) https://eur-lex.europa.eu/eli/reg/2024/2847/oj/itahttps://eur-lex.europa.eu/eli/reg/2024/2847/oj/ita; regolamento (UE) 2017/745 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medici https://eur-lex.europa.eu/eli/reg/2017/745/oj/itahttps://eur-lex.europa.eu/eli/reg/2017/745/oj/ita (regolamento relativo ai dispositivi medici), https://eur-lex.europa.eu/eli/reg/2017/745/oj/ita (il regolamento relativo ai dispositivi medici); regolamento (UE) 2017/746 del Parlamento europeo e del Consiglio, del 5 aprile 2017, relativo ai dispositivi medico-diagnostici in vitro (regolamento relativo ai dispositivi medico-diagnostici in vitro) https://eur-lex.europa.eu/eli/reg/2017/746/oj/itahttps://eur-lex.europa.eu/eli/reg/2017/746/oj/ita; regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (regolamento generale sulla protezione dei dati), https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32016R0679https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32016R0679; regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio, del 13 giugno 2024, che stabilisce regole armonizzate sull'intelligenza artificiale (regolamento sull'intelligenza artificiale), https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32024R1689; proposta di regolamento del Parlamento europeo e del Consiglio sullo spazio europeo dei dati sanitari (COM(2022) 197 final), https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:52022PC0197. I negoziati si sono conclusi con un accordo politico nella primavera del 2024 e la pubblicazione nella Gazzetta ufficiale è prevista, previa finalizzazione, per la primavera 2025.

normativa in materia di cibersicurezza, ad esempio fornendo orientamenti attuativi[27] e, ove necessario, promuovendo norme pertinenti.

I futuri **portafogli europei di identità digitale** sono un altro strumento inteso a facilitare la semplice attuazione di buone pratiche di igiene informatica. Ridurre il ricorso a meccanismi di identificazione deboli, come le password, è essenziale per attenuare i rischi di accesso non autorizzato ai dati sanitari. Il passaggio a soluzioni sicure di accesso basate su un'identificazione affidabile è fondamentale. Il portafoglio di identità digitale dell'UE offre un approccio armonizzato a livello di UE all'identificazione elettronica per gli operatori sanitari, fornendo una soluzione robusta e unificata a partire dalla fine del 2026. Per tutti i sistemi di informazione sanitaria online tenuti a implementare l'autenticazione forte dell'utente vigerà l'obbligo di accettare il portafoglio a fini di identificazione a partire dalla fine del 2027[28].

Preparazione e sostegno mirato

La verifica della preparazione, che prevede azioni quali i test di penetrazione, è una pietra angolare di una cibersicurezza efficace e la Commissione ha già stanziato finanziamenti all'ENISA per iniziative pilota di preparazione, dalle quali è emerso che il settore sanitario è uno dei settori in cui è più elevata la richiesta di test e di ulteriori valutazioni per individuare le lacune nella maturità della cibersicurezza. Con l'entrata in vigore del regolamento sulla cibersolidarietà aumenteranno in modo significativo gli sforzi di questo tipo, nel cui ambito un ruolo guida sarà assunto dall'ECCC. Per rispondere a tale necessità, la Commissione proporrà, in consultazione con gruppo di cooperazione NIS, EU-CyCLONe[29] e ENISA, di identificare la sanità come settore al quale può essere fornito sostegno ai fini della **verifica coordinata della preparazione** a norma del regolamento sulla cibersolidarietà. Inoltre il centro di sostegno dovrebbe elaborare un **quadro su misura per le valutazioni di maturità della cibersicurezza specifico per l'assistenza sanitaria**. Tali valutazioni di maturità fornirebbero ai soggetti conoscenze utili sulle loro vulnerabilità, consentendo loro nel contempo di dimostrare ai pazienti e ai portatori di interessi la loro preparazione in materia di cibersicurezza e consolidando così la fiducia nei loro servizi. A livello aggregato il centro di sostegno dovrebbe effettuare una **valutazione annuale di maturità della cibersicurezza in ambito sanitario**, che fornirebbe una panoramica chiara della cibersicurezza nel settore sanitario a livello sia nazionale sia di UE.

Il settore sanitario fa ampio affidamento su contraenti esterni per i servizi di cibersicurezza[30], il che sottolinea la necessità di un sostegno mirato per rafforzare le difese. Sulla base di iniziative efficaci quali i voucher per l'innovazione dell'UE, gli **Stati membri dovrebbero prendere in considerazione misure mirate come i voucher per la cibersicurezza per le micro, piccole e medie strutture ospedaliere e di**

[27] L'elaborazione di orientamenti sull'interpretazione del regolamento generale sulla protezione dei dati è di competenza del comitato europeo per la protezione dei dati (*European Data Protection Board*, EDPB). L'elaborazione di orientamenti da parte dell'ENISA dovrebbe avvenire nel pieno rispetto delle prerogative dell'EDPB.
[28] Articolo 5 septies, paragrafi 1 e 2, del regolamento (UE) n. 910/2014.
[29] Rete europea delle organizzazioni di collegamento per le crisi informatiche.
[30] Cfr. il documento *NIS Investments Report 2023* dell'ENISA (novembre 2023), nel quale è evidenziata l'importanza del sostegno esterno per l'audit e la conformità in materia di cibersicurezza. Disponibile all'indirizzo https://www.enisa.europa.eu/publications/nis-investments-2023.

prestazione di assistenza sanitaria. Tali voucher fornirebbero un'assistenza finanziaria ai fini dell'attuazione di specifiche misure di cibersicurezza. La definizione delle priorità nell'assegnazione dei voucher dovrebbe basarsi sui risultati della verifica della preparazione e delle valutazioni di maturità.

Le conoscenze e il contesto locali sono fondamentali per un'introduzione efficace dei voucher o di altri programmi di sostegno, garantendone pertinenza e accessibilità. I fondi dell'UE, come il Fondo europeo di sviluppo regionale, sono già attivi nel sostenere le iniziative in materia di cibersicurezza e sanità digitale e potrebbero pertanto costituire un veicolo di sviluppo di sistemi mirati di voucher per la cibersicurezza destinati ai prestatori di assistenza sanitaria. Al fine di guidare questa operazione il centro di sostegno collaborerebbe con gli Stati membri e le autorità dei programmi regionali per sostenere lo sviluppo di tali sistemi regionali di voucher, traendo spunto dagli insegnamenti tratti dai progetti nazionali esistenti e dalle azioni finanziate nell'ambito del programma Europa digitale per garantire un'attuazione pratica e incisiva.

Inoltre, dal 2014 i programmi Orizzonte sono stati determinanti per finanziare una serie di iniziative di ricerca incentrate sul rafforzamento della resilienza delle istituzioni sanitarie, come gli ospedali, a fronte delle minacce informatiche e sull'attenuazione dei rischi associati all'uso improprio delle tecnologie emergenti. I risultati ottenuti comprendono una serie di strumenti, quadri e sistemi specializzati, quali strumenti di valutazione del rischio, piattaforme di condivisione dei dati che tutelano la privacy, soluzioni crittografiche, programmi di formazione per la sensibilizzazione alla cibersicurezza e sistemi di rilevamento delle minacce in tempo reale. Tali soluzioni sono state, in particolare, rigorosamente convalidate attraverso attuazioni pilota reali negli ambienti sanitari, a garanzia della loro efficacia e applicabilità pratica nella protezione dalle minacce informatiche.

Garantire la sicurezza delle catene di approvvigionamento dell'assistenza sanitaria

Una sfida fondamentale per le organizzazioni sanitarie è la gestione di complesse catene di approvvigionamento delle TIC, che riguardano una serie di prodotti quali dispositivi medici connessi, sistemi per le cartelle cliniche elettroniche e hardware per gli uffici. Gli ospedali e i prestatori di assistenza sanitaria necessitano di sistemi e servizi TIC affidabili e sicuri per il loro funzionamento. Per contribuire ad affrontare le sfide di cibersicurezza nel settore sanitario, il gruppo di cooperazione NIS dovrebbe effettuare una **valutazione coordinata dei rischi per la sicurezza, valutando i rischi sia tecnici che strategici connessi alle catene di approvvigionamento dei dispositivi medici e proponendo misure di attenuazione**[31]. Ove opportuno, il gruppo di cooperazione NIS dovrebbe collaborare con il gruppo di coordinamento per i dispositivi medici.

Il regolamento sulla ciberresilienza costituisce un nuovo quadro globale che stabilisce requisiti di cibersicurezza per la pianificazione, la progettazione e lo sviluppo, comprese la gestione, la risoluzione mediante patch e la segnalazione delle vulnerabilità attivamente sfruttate, in relazione a quasi tutti i prodotti hardware e software, in ogni fase della catena del valore[32]. I dispositivi medici sono un tipo di

[31] A norma dell'articolo 22 della direttiva NIS 2.

[32] In una prima fase, a partire dal 1º agosto 2025, ampie categorie di apparecchiature radio, che non rientrano nell'ambito di applicazione del regolamento relativo ai dispositivi medici e del regolamento relativo ai dispositivi medico-diagnostici in

prodotto utilizzato in uno dei settori più sensibili della nostra società. I requisiti di cibersicurezza per tali prodotti derivano da due regolamenti preesistenti: il regolamento relativo ai dispositivi medici e il regolamento relativo ai dispositivi medico-diagnostici in vitro[33]. La valutazione attualmente in corso di tali regolamenti sta esaminando le possibilità di aumento della coerenza e delle sinergie tra tali quadri al fine di garantire la semplificazione e una cibersicurezza all'avanguardia.

I risultati della valutazione dei rischi dovrebbero inoltre aiutare le organizzazioni sanitarie a rivedere le loro pratiche di cibersicurezza delle catene di approvvigionamento, come previsto dalla direttiva NIS 2, e potrebbero orientare l'elaborazione di nuovi **orientamenti in materia di appalti**[34]. Elaborati dall'ENISA mediante il suo centro di sostegno, tali orientamenti dovrebbero riflettere le tendenze recenti, come la cloudificazione dell'archiviazione dei dati dei pazienti, compresa la necessità di una migrazione sicura dei dati sanitari elettronici verso ambienti cloud. I nuovi orientamenti dovrebbero inoltre offrire alle organizzazioni strumenti pratici per tenere traccia delle loro catene di approvvigionamento, compresi i fornitori di servizi di sicurezza gestiti, le relazioni di attestazione o le valutazioni dei rischi da parte di terzi.

Per quanto riguarda il cloud, sono necessarie ulteriori azioni per affrontare le sfide uniche derivanti dalla gestione dei dati sanitari sensibili, tra cui la necessità di una maggiore sicurezza, la privacy e i rischi operativi. Per rafforzare le garanzie, gli esperti raccomandano di integrare la "sicurezza predefinita e fin dalla progettazione" nei servizi cloud. Questo approccio privilegia le infrastrutture sicure, la gestione proattiva delle vulnerabilità e una combinazione di soluzioni cloud governative e private. Per garantire solide pratiche di sicurezza sono inoltre essenziali il monitoraggio continuo e gli attestati specifici dei fornitori di servizi di sicurezza, quali le certificazioni dei fornitori di sicurezza e i controlli di conformità alle norme nazionali e internazionali.

Per i servizi a livello di infrastruttura (*Infrastructure-as-a-Service* – IaaS), i servizi a livello di piattaforma (*Platform-as-a-Service* – PaaS) e i servizi a livello di software (*Software-as-a-Service* – SaaS), l'attuazione delle misure di sicurezza spesso ricade sul cliente. Tuttavia molte organizzazioni sanitarie non dispongono delle risorse necessarie per soddisfare tali requisiti in modo indipendente. Per far fronte a questo problema, **i fornitori di servizi cloud dovrebbero essere incoraggiati ad attuare misure di sicurezza di base come caratteristica standard**. Tali misure ridurrebbero il rischio di configurazioni errate, manterrebbero una protezione costante in tutti gli ambienti gestiti dai clienti e fornirebbero maggiori garanzie agli utenti. Lo scopo della definizione di un livello di base predefinito per la sicurezza sarebbe bilanciare protezione robusta e praticità, garantendo l'usabilità per un'ampia gamma di organizzazioni sanitarie. Questo sforzo richiederebbe una stretta collaborazione tra i fornitori

vitro, saranno tenute a rispettare, al momento della loro immissione sul mercato unico, i requisiti essenziali relativi alla cibersicurezza della direttiva sulle apparecchiature radio. In una seconda fase, a partire dall'11 dicembre 2027, entrerà in vigore il regolamento sulla ciberresilienza.

[33] Nel dicembre 2019 il gruppo di cooperazione per i dispositivi medici ha pubblicato orientamenti sulla cibersicurezza per i dispositivi medici, volti ad aiutare fabbricanti a soddisfare i requisiti di cui all'allegato I dei due regolamenti: https://ec.europa.eu/docsroom/documents/41863?locale=it.

[34] Sulla base degli orientamenti dell'ENISA del 2020 in materia di appalti per la cibersicurezza negli ospedali (*Procurement Guidelines for Cybersecurity in Hospitals* - febbraio 2020). Disponibili all'indirizzo https://www.enisa.europa.eu/publications/good-practices-for-the-security-of-healthcare-services

di servizi cloud e il settore sanitario, allo scopo di sfruttare le migliori pratiche dell'industria per creare soluzioni efficaci e scalabili.

Formazione e sviluppo delle competenze

Disporre di personale dotato delle competenze più richieste è importante per la crescita sostenibile e la competitività a lungo termine in Europa, come anche per offrire servizi di alta qualità, compresi i servizi sanitari. La carenza di professionisti della cibersicurezza qualificati rappresenta una sfida significativa in tutta Europa; si stima che manchino 299 000 professionisti per soddisfare le esigenze di personale dell'UE nel settore[35]. Secondo l'Eurobarometro del 2024 sulle competenze in materia di cibersicurezza[36], l'81 % delle imprese ritiene che le difficoltà nell'assunzione di personale addetto alla cibersicurezza costituiscano un rischio fondamentale per potenziali attacchi informatici. Nei settori dell'istruzione, della sanità e dell'assistenza sociale, il 66 % dei ruoli di cibersicurezza è ricoperto da dipendenti che vengono da posizioni non legate alla cibersicurezza, il che evidenzia l'urgente necessità di riqualificazione e miglioramento del livello delle competenze.

Per affrontare questa sfida, il centro di sostegno dovrebbe collaborare con il futuro consorzio per l'infrastruttura digitale europea (EDIC) per le competenze in materia di cibersicurezza, previsto nella comunicazione della Commissione sull'Accademia per le competenze in materia di cibersicurezza[37]. Ciò dovrebbe facilitare gli scambi tra i professionisti della cibersicurezza nel settore sanitario, quali i responsabili della sicurezza informatica (*Chief Information Security Officers* - CISO). Una potenziale iniziativa potrebbe essere la creazione, partendo da un gruppo di esperti, di **una rete europea dei CISO del settore sanitario**, per la condivisione e lo sviluppo di migliori pratiche, strategie di mantenimento dei talenti e soluzioni per attrarre professionisti della cibersicurezza verso il settore sanitario. Nell'ambito dell'Accademia per le competenze in materia di cibersicurezza dovrebbero inoltre essere sviluppate risorse finalizzate a aumentare la disponibilità di personale specializzato in cibersicurezza in ambito sanitario con il sostegno dell'industria e del mondo accademico. A tale riguardo, i portatori di interessi del settore dovrebbero essere incoraggiati a impegnarsi a sostenere un aumento dell'offerta di formazione in materia di cibersicurezza.

L'errore umano continua a essere uno dei principali fattori che contribuiscono agli incidenti di cibersicurezza nell'assistenza sanitaria, il che sottolinea la fondamentale necessità di una formazione completa del personale e di una sensibilizzazione in materia di cibersicurezza. Dato l'uso frequente di strumenti digitali da parte degli operatori sanitari, è essenziale che questi ultimi conoscano le pratiche sicure. La formazione mirata e le campagne di sensibilizzazione possono ridurre i rischi in modo significativo. A tal fine il centro di sostegno dovrebbe lavorare insieme agli operatori sanitari e ai

[35] *The 2024 cybersecurity landscape: insights from the ISC2 cybersecurity workforce study | Digital Skills and Jobs Platform* (Piattaforma per le competenze e le occupazioni digitali)

[36] Eurobarometro Flash 547 sulle competenze in materia di cibersicurezza.

[37] Comunicazione della Commissione al Parlamento europeo e al Consiglio - Colmare il divario di talenti nel settore della cibersicurezza per rafforzare la competitività, la crescita e la resilienza dell'UE ("Accademia per le competenze in materia di cibersicurezza") (COM(2023) 207 final).

prestatori di assistenza sanitaria e cooperare con gli erogatori di istruzione e formazione, l'industria, l'EDIC per le competenze in materia di cibersicurezza e le autorità degli Stati membri per creare e diffondere **moduli e corsi di formazione online di ampio respiro e di facile accesso**.

L'integrazione delle competenze digitali e dei moduli di cibersicurezza nei programmi di studio è fondamentale per costruire una solida base in materia di cibersicurezza nell'assistenza sanitaria. Tali moduli dovrebbero affrontare questioni settoriali specifiche come la protezione dei dati dei pazienti e le vulnerabilità nella sicurezza dei dispositivi medici. Lo sviluppo di tali risorse dovrebbe tenere conto di azioni precedenti, come il progetto BeWell finanziato nell'ambito del programma Erasmus+[38] e il progetto PANACEA finanziato nell'ambito di Orizzonte 2020[39].

3.2. Capacità europee di rilevamento delle minacce informatiche dirette al settore sanitario

Un rilevamento efficace delle minacce informatiche è essenziale per una risposta rapida agli incidenti. Gli autori delle minacce possono sfruttare tecniche volte a rendere le intrusioni difficili da rilevare, che consentono l'accesso non autorizzato a un sistema per periodi di tempo prolungati[40]. Migliori capacità di rilevamento delle minacce possono pertanto contribuire a fermare tempestivamente gli attacchi informatici. Ad esempio, nell'attacco ransomware contro il fornitore finlandese di servizi di psicoterapia Vastaamo, durante il quale sono state rubate le cartelle cliniche riservate dei pazienti, l'intrusione iniziale si è verificata nel 2018, ma il fornitore ne è venuto a conoscenza solo nel 2020[41].

Una condivisione delle informazioni e una collaborazione efficienti sono essenziali per migliorare il rilevamento delle minacce e la conoscenza situazionale nell'UE. I gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT) svolgono un ruolo fondamentale nel ricevere segnalazioni di incidenti, quasi incidenti e potenziali minacce, offrendo orientamenti sulle misure di attenuazione a livello nazionale. Tuttavia **gli Stati membri sono fortemente incoraggiati a condividere con il centro di sostegno dell'ENISA anche tutte le segnalazioni di incidenti informatici inviate dagli ospedali e dai prestatori di assistenza sanitaria, per consentire una conoscenza situazionale nell'UE**. Ciò dovrebbe idealmente essere accompagnato da una caratterizzazione significativa dei diversi aspetti rilevanti degli incidenti, comprese le vulnerabilità di fondo note, gli effetti sui servizi sanitari e gli eventi avversi per i pazienti. I fabbricanti di dispositivi medici e medico-diagnostici in vitro sono inoltre incoraggiati a segnalare volontariamente, attraverso la piattaforma unica di segnalazione che sarà istituita e gestita dall'ENISA nel quadro del regolamento sulla ciberresilienza, le vulnerabilità attivamente sfruttate o gli incidenti informatici gravi che hanno un impatto sulla sicurezza di tali dispositivi e

[38] BeWell – *Blueprint Alliance for a future health workforce strategy on digital and green skills* (Progetto di alleanza per una futura strategia in materia di competenze digitali e verdi per il personale sanitario). Disponibile all'indirizzo https://bewell-project.eu/.
[39] PANACEA – *Protection and privAcy of hospital and health iNfrastructures with smArt Cyber sEcurity and cyber threat toolkit for data and people* (Protezione e privacy delle infrastrutture ospedaliere e sanitarie con strumenti intelligenti per la cibersicurezza e le minacce informatiche per i dati e le persone). Disponibile all'indirizzo https://cordis.europa.eu/project/id/826293.
[40] Relazione dell'ENISA sul panorama delle minacce 2023.
[41] Decisione 1150/161/2021 del garante finlandese per la protezione dei dati.

possibilmente anche altre vulnerabilità, incidenti, quasi incidenti o minacce informatiche che possono incidere sul profilo di rischio di tali dispositivi.

Una volta che le informazioni contenute nelle relazioni non saranno più sensibili, il centro di sostegno potrebbe creare un catalogo europeo, sponsorizzato dall'ENISA, delle vulnerabilità note sfruttate per i dispositivi medici, i sistemi di cartelle cliniche elettroniche e i fornitori di apparecchiature e software TIC nel settore sanitario. Per affrontare le sfide significative dell'individuazione delle minacce, il centro di sostegno dovrebbe introdurre **un servizio di allarme rapido a livello di UE per il settore sanitario accessibile tramite iscrizione, che fornisca allerte in tempo quasi reale**. Tale servizio si baserebbe sui dati trattati provenienti dai CSIRT, dagli enti sanitari, dai fabbricanti, dall'OSINT (*Open-Source Intelligence*) e da altri attori pertinenti quali i poli informatici, i centri di condivisione e analisi delle informazioni (ISAC) e le autorità di contrasto. Una cooperazione rafforzata tra l'ENISA e l'Agenzia dell'Unione europea per la cooperazione nell'attività di contrasto (Europol) - ad esempio sulle forme di criminalità informatica che prendono di mira il settore sanitario - rafforzerebbe ulteriormente la conoscenza situazionale.

Gli ISAC fungono da risorse centrali per l'intelligence sulle minacce informatiche, agevolando lo scambio di informazioni bidirezionale tra il settore pubblico e quello privato e promuovendo la creazione di fiducia. Il centro di sostegno dovrebbe contribuire ulteriormente all'**ISAC europeo per il settore sanitario** mediante strumenti, scambi di informazioni e relazioni sulla conoscenza situazionale settoriale, nonché promuovendo una comunità affidabile per la collaborazione tattica e strategica. Gli Stati membri dovrebbero incentivare lo sviluppo di ISAC nazionali per il settore sanitario[42]. Gli ISAC dovrebbero inoltre essere incoraggiati a riunire i prestatori di assistenza sanitaria e i fabbricanti per dar luogo a una comprensione congiunta delle minacce alla cibersicurezza, anche nella catena di approvvigionamento, e facilitare un dialogo sulla progettazione sicura dei prodotti che tenga realmente conto delle realtà dell'implementazione sul campo.

3.3.Risposta e ripresa rapide

Data l'elevata sensibilità dei dati sanitari dei pazienti e gli effetti potenzialmente devastanti degli attacchi informatici sui servizi sanitari, una risposta rapida ed efficace agli incidenti di cibersicurezza è fondamentale per salvaguardare la sicurezza dei pazienti. Quando un ospedale o un prestatore di assistenza sanitaria si trova di fronte a un attacco informatico, il primo punto di contatto è il CSIRT nazionale pertinente[43]. Il CSIRT ha il compito di fornire un sostegno tempestivo, idealmente entro 24

[42] La Finlandia, ad esempio, dispone di un ISAC nazionale per il settore dei servizi sociali e dell'assistenza sanitaria. Cfr. Centro nazionale finlandese per la cibersicurezza: "*ISAC information sharing groups*", disponibile all'indirizzo https://www.kyberturvallisuuskeskus.fi/en/our-services/situation-awareness-and-network-management/isac-information-sharing-groups.

[43] L'articolo 23, paragrafo 1, della direttiva NIS 2 stabilisce l'obbligo per i soggetti essenziali e importanti di notificare gli incidenti significativi al CSIRT pertinente o, se del caso, all'autorità competente.

ore, per contribuire alla gestione degli incidenti significativi. Tuttavia, se un incidente supera le capacità del CSIRT, dovrebbe essere disponibile il sostegno dell'UE per garantire una risposta rapida ed efficace.

La riserva dell'UE per la cibersicurezza, istituita a norma del regolamento sulla cibersolidarietà, prevede servizi di risposta agli incidenti erogati da fornitori di fiducia di servizi di sicurezza gestiti per fornire assistenza in caso di incidenti di cibersicurezza significativi o su vasta scala e negli sforzi di ripresa iniziali. Tale riserva è intesa a integrare gli sforzi dei CSIRT degli Stati membri, consentendo loro di richiedere un sostegno supplementare nei casi che coinvolgono settori critici come la sanità. Per rafforzare tale sistema, la **Commissione e l'ENISA dovrebbero garantire che la riserva comprenda un servizio di risposta rapida specifico per il settore sanitario.** In complementarità con altri quadri esistenti, tale servizio consentirebbe di inviare esperti per gestire tempestivamente incidenti di cibersicurezza significativi o su vasta scala nel settore dell'assistenza sanitaria, quando il sostegno nazionale è insufficiente.

Per migliorare la risposta e la ripresa, il centro di sostegno, in collaborazione con il gruppo di cooperazione NIS, la rete di CSIRT e, ove pertinente, Europol, dovrebbe elaborare **protocolli per la risposta agli incidenti informatici specifici per l'assistenza sanitaria**. Tali protocolli guiderebbero sia i CSIRT che le organizzazioni sanitarie nella risposta a specifiche minacce alla cibersicurezza, ransomware inclusi. Data l'importanza di una cooperazione efficace tra i CSIRT e le autorità di contrasto nella risposta agli incidenti di cibersicurezza di natura criminale e nelle indagini sugli stessi, i protocolli dovrebbero fornire, tra l'altro, orientamenti chiari sulla segnalazione di tali incidenti alle autorità di contrasto. Il centro di sostegno potrebbe inoltre **facilitare l'esecuzione di ampie esercitazioni nazionali di cibersicurezza, basandosi sull'esperienza maturata durante esercitazioni come Cyber Europe 2022 dell'ENISA, per testare i protocolli e rafforzare la risposta agli incidenti.**

Per orientare le politiche e valutare l'efficacia delle misure adottate contro gli attacchi ransomware, è necessario raccogliere ulteriori dati. A tal fine gli Stati membri dovrebbero chiedere ai soggetti interessati dalla direttiva NIS 2, comprese le organizzazioni sanitarie, di dichiarare gli eventuali pagamenti di riscatto effettuati e che si intendono effettuare, in aggiunta alle altre informazioni fornite al momento della segnalazione di incidenti di cibersicurezza significativi. Ciò contribuirebbe a indagini efficaci sugli incidenti con uso di ransomware, ad esempio rendendo possibile il tracciamento dei pagamenti sulle piattaforme di scambio di criptovalute al fine di identificare i destinatari.

La velocità di ripresa è un fattore cruciale per il mantenimento della resilienza e della fiducia dei cittadini, in particolare nell'assistenza sanitaria, dove i tempi di inattività possono creare perturbare l'assistenza ai pazienti. Per una ripresa efficace dagli attacchi ransomware, i prestatori di assistenza sanitaria devono disporre di backup sicuri, aggiornati e isolati che possano essere rapidamente ripristinati. Nell'ambito del suo catalogo dei servizi, il centro di sostegno potrebbe offrire un **servizio, accessibile tramite iscrizione, di ripresa da un attacco ransomware, che aiuti gli ospedali e i prestatori di assistenza sanitaria a preparare in anticipo i piani di ripresa**. ENISA e Europol dovrebbero collaborare per individuare i ceppi ransomware più comuni con cui sono prese di mira le organizzazioni sanitarie e **ampliare l'archivio degli strumenti di decrittazione** disponibili attraverso il progetto "No More Ransom"[44] e

[44] https://www.nomoreransom.org/it/index.html.

dovrebbero inoltre sviluppare e promuovere orientamenti accessibili per aiutare i prestatori di assistenza sanitaria a evitare il pagamento di riscatti utilizzando tali strumenti di decrittazione.

L'**iniziativa internazionale "Counter Ransomware"**[45] costituisce una valida piattaforma per gli scambi su specifici incidenti ransomware e contribuisce a sostenere i paesi membri nel rafforzamento dei quadri di cibersicurezza e delle capacità di svolgere indagini nei confronti degli autori dei ransomware. La Commissione, in collaborazione con l'alto rappresentante, proseguirà la collaborazione nell'ambito dell'iniziativa "Counter Ransomware", anche contro le minacce ransomware al settore sanitario. La Commissione cercherà inoltre di cooperare nell'ambito del **gruppo di lavoro del G7 sulla cibersicurezza** per rafforzare la cibersicurezza del settore sanitario. In particolare, il gruppo di lavoro potrebbe valutare le possibilità di sostegno al settore sanitario contro le minacce anche ransomware, basandosi su riflessioni come quelle contenute nella dichiarazione congiunta sugli attacchi ransomware contro le strutture sanitarie dell'8 novembre 2024 presentata nel contesto del Consiglio di sicurezza delle Nazioni Unite[46].

4. Azioni a livello nazionale

La capacità del presente piano d'azione di migliorare la cibersicurezza nel settore sanitario dipende dal coinvolgimento attivo e dall'impegno degli Stati membri. Per attuare con successo il piano d'azione, gli Stati membri potrebbero designare **centri nazionali di sostegno alla cibersicurezza dedicati specificamente agli ospedali e ai prestatori di assistenza sanitaria**. Tali centri costituirebbero i punti di contatto primari per il settore sanitario a livello nazionale, collaborando strettamente con il centro di sostegno dell'ENISA. Ove possibile e pertinente, gli Stati membri dovrebbero designare quali centri nazionali di sostegno alla cibersicurezza organismi esistenti, come i CSIRT sanitari nazionali o le autorità pertinenti.

Gli Stati membri sono inoltre incoraggiati a elaborare **piani d'azione nazionali incentrati sulla cibersicurezza nel settore sanitario**. Tali piani dovrebbero delineare i rischi di cibersicurezza specifici cui sono esposti i sistemi sanitari e le azioni nazionali intraprese per affrontarli, garantendo nel contempo che le risorse e le pratiche a livello europeo siano utilizzate in modo efficace. Il centro di sostegno dell'ENISA può fornire assistenza nell'elaborazione di tali piani, tenendo conto dei piani nazionali già esistenti e coordinando gli sforzi per garantire che le risorse e le strategie dei singoli Stati membri si completino a vicenda.

Un altro obiettivo fondamentale per gli Stati membri è facilitare la condivisione delle risorse tra i prestatori di assistenza sanitaria, che potrebbe essere conseguita mediante **appalti congiunti o la messa in comune di risorse** a livello regionale, nazionale o persino europeo. Tale approccio ridurrebbe l'onere

[45] https://www.counter-ransomware.org/.
[46] https://usun.usmission.gov/joint-statement-on-ransomware-attacks-against-healthcare-facilities/.

finanziario per i singoli soggetti, aumentando nel contempo il loro potere contrattuale con i fornitori di servizi di cibersicurezza.

Ad esempio, il programma francese CaRE[47] ha introdotto una serie di misure a livello nazionale e regionale per affrontare le sfide in materia di risorse: un catalogo informatico fornisce una panoramica delle soluzioni e dei pacchetti di cibersicurezza a disposizione degli ospedali attraverso l'agenzia nazionale per la cibersicurezza, l'agenzia per la sanità digitale, le agenzie regionali, le organizzazioni nazionali di acquisto e le soluzioni commerciali. A ciò si aggiungono finanziamenti supplementari destinati alle agenzie regionali affinché offrano risorse condivise.

Gli Stati membri dovrebbero inoltre affrontare la questione dei livelli di investimenti insufficienti nella cibersicurezza del settore sanitario. Per garantire finanziamenti adeguati, dovrebbero fissare **parametri di riferimento non vincolanti e monitorare gli obiettivi di finanziamento specificamente destinati alla cibersicurezza**, garantendo nel contempo che tali investimenti non compromettano i servizi essenziali di assistenza ai pazienti. Tali obiettivi di finanziamento dovrebbero inoltre mirare a integrare considerazioni di sicurezza in tutti gli investimenti digitali del settore. Gli Stati membri possono scambiarsi migliori pratiche e consulenze su tali obiettivi attraverso piattaforme quali la rete di assistenza sanitaria on line[48].

5. Cooperazione pubblico-privato

La cooperazione pubblico-privato e la consultazione con i prestatori di assistenza sanitaria, gli altri soggetti del settore sanitario e i pertinenti operatori del settore della cibersicurezza sono essenziali per l'efficace attuazione del piano d'azione. Per contribuire ulteriormente ai lavori del centro di sostegno, la **Commissione, con il sostegno dell'ENISA, istituirà un comitato consultivo comune per la cibersicurezza del settore sanitario** con rappresentanti di alto livello dei settori dell'assistenza sanitaria e della cibersicurezza, che potrà fornire consulenza alla Commissione e al centro di sostegno su azioni incisive e discuterà l'ulteriore sviluppo di partenariati pubblico-privato in questo campo. Il comitato sfrutterà le opportunità esistenti per i partenariati pubblico-privato, compreso l'ISAC europeo per il settore sanitario.

La Commissione pubblicherà inoltre un **invito ad agire** destinato a imprese, fondazioni, istituti di istruzione e portatori di interessi del settore della cibersicurezza affinché **si impegnino ad adottare misure per affrontare le sfide del settore**. Sfruttando l'esperienza dell'Accademia per le competenze in materia di cibersicurezza, tali impegni potrebbero, ad esempio, portare all'inclusione nell'ambito di tale Accademia dell'offerta di corsi di formazione e materiali per i professionisti della cibersicurezza dedicati specificamente al settore sanitario[49]. Altri impegni potrebbero riguardare anche le attività di

[47] Agenzia francese per la sanità digitale: *Cybersécurité acceleration et Résilience des Établissements* (CaRE). Disponibile all'indirizzo https://esante.gouv.fr/strategie-nationale/cybersecurite.
[48] La rete di assistenza sanitaria on line (*eHealth*) è una rete volontaria che collega le autorità nazionali responsabili dell'assistenza sanitaria online designate dagli Stati membri, istituita sulla base dell'articolo 14 della direttiva 2011/24/UE.
[49] Cyber Skills Academy: Get Involved | Digital Skills and Jobs Platform (Piattaforma per le competenze e le occupazioni digitali)

sensibilizzazione o l'erogazione gratuita o a costi ridotti di servizi di sicurezza gestiti a soggetti particolarmente vulnerabili, al fine di aumentarne la preparazione e la resilienza in materia di cibersicurezza. Gli impegni potrebbero inoltre consistere nella condivisione di intelligence sulle minacce informatiche con il centro di sostegno dell'ENISA. Il centro di sostegno dovrebbe mantenere una visione globale degli impegni assunti nell'ambito dell'invito ad agire, con l'obiettivo di garantirne la coerenza e la complementarità.

6. Scoraggiare gli autori delle minacce informatiche

Le politiche interne ed esterne dell'UE in materia di cibersicurezza dovrebbero sostenere l'obiettivo di scoraggiare gli autori delle minacce informatiche dall'attaccare i sistemi sanitari europei. Gli attacchi informatici contro le organizzazioni sanitarie sono un tipo di attività informatica dolosa particolarmente inaccettabile, data la loro capacità di minacciare la sicurezza dei pazienti e mettere in pericolo le vite umane. Pertanto le capacità di deterrenza dell'UE nel settore della cibersicurezza e delle attività di contrasto dovrebbero essere sfruttate al massimo, al fine di minare il modello di business generale degli autori delle minacce dirette al settore sanitario e privarli di profitti facili. Ciò includerebbe la promozione delle indagini transfrontaliere, mediante una migliore condivisione degli indicatori di compromissione e di altri dati pertinenti, e una maggiore attenzione verso gli obiettivi di valore elevato e i servizi chiave che facilitano le attività illegali, quali i servizi di bulletproof hosting o quelli che consentono di mescolare le criptovalute.

Il **pacchetto di strumenti della diplomazia informatica** offre un quadro per prevenire, scoraggiare e rispondere agli attacchi informatici contro l'UE, gli Stati membri e i partner. L'alto rappresentante continuerà a utilizzare l'attuale quadro di sanzioni contro gli attacchi informatici per rispondere alle minacce rivolte ai sistemi sanitari.

Far sì che i criminali siano ritenuti responsabili delle loro azioni costituisce un importante deterrente. Gli Stati membri dovrebbero quindi garantire che le attività di contrasto siano pienamente integrate nei rispettivi piani d'azione nazionali. In particolare, per scoraggiare gli attacchi, consegnare i criminali alla giustizia e smantellare le infrastrutture criminali che facilitano gli attacchi, dovrebbero avvalersi appieno delle disposizioni della direttiva relativa agli attacchi contro i sistemi di informazione[50] e della Convenzione del Consiglio d'Europa sulla criminalità informatica conclusa a Budapest[51]. L'efficace attuazione di tali strumenti dovrebbe garantire che le azioni criminali e dolose contro l'assistenza sanitaria siano punite.

7. Attuazione e monitoraggio del piano d'azione

Nel presente piano d'azione è stata individuata una serie di compiti per un centro di sostegno da istituire nell'ambito dell'ENISA, al fine di garantire un'attuazione globale e coerente del piano d'azione, evitando

[50] Direttiva 2013/40/UE del Parlamento europeo e del Consiglio, del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio: https://eur-lex.europa.eu/eli/dir/2013/40/oj/ita

[51] Convenzione sulla criminalità informatica (Convenzione di Budapest, STCE n. 185) e relativi protocolli: https://www.coe.int/en/web/cybercrime/the-budapest-convention

nel contempo la creazione di nuovi enti, che potrebbe portare a potenziali sovrapposizioni e costi generali. La Commissione intende provvedere affinché il centro di sostegno disponga di risorse adeguate.

Il consiglio di amministrazione dell'ENISA e le reti pertinenti degli Stati membri, in particolare il gruppo di cooperazione NIS, la rete di CSIRT, la rete di assistenza sanitaria on line e, ove pertinente, il comitato dello spazio europeo dei dati sanitari dovrebbero essere periodicamente informati dall'ENISA, in consultazione con la Commissione, sulle attività di tale centro di sostegno, una volta che sarà operativo. L'ENISA dovrebbe inoltre procedere a uno scambio continuo con il comitato consultivo pubblico-privato per la cibersicurezza nel settore sanitario in merito all'attuazione delle azioni fornite dal centro di sostegno.

Le relazioni periodiche dell'ENISA, come la relazione sullo stato della cibersicurezza nell'Unione, che fornisce una valutazione aggregata del livello di maturità delle capacità e delle risorse di cibersicurezza in tutta l'UE, anche nel settore sanitario, dovrebbero rappresentare un'occasione per pubblicare dati pertinenti, a sostegno del monitoraggio del piano d'azione. L'indice della cibersicurezza dell'UE elaborato dall'ENISA[52] può inoltre fornire dati quantitativi e qualitativi, che possono essere utilizzati per valutare le criticità e la maturità del settore sanitario.

8. Prossime tappe

La presente comunicazione definisce un'agenda ambiziosa per una maggiore cibersicurezza del settore sanitario dell'UE. Proponendo l'istituzione di un centro di sostegno alla cibersicurezza per gli ospedali e i prestatori di assistenza sanitaria nel cuore dell'ENISA, il piano d'azione traccia la strada verso la definizione di un approccio europeo coerente e condiviso alle sfide di cibersicurezza in tale settore.

La presente comunicazione dovrebbe essere considerata l'inizio di un processo volto a migliorare la cibersicurezza nel settore sanitario. L'adozione del piano d'azione sarà pertanto accompagnata dall'avvio di ampie consultazioni dei portatori di interessi e dal proseguimento degli scambi con gli Stati membri e le reti pertinenti per raccogliere informazioni. Sulla base dei risultati delle consultazioni, la Commissione intende presentare raccomandazioni nel quarto trimestre del 2025, al fine di perfezionare ulteriormente il piano d'azione.

La Commissione invita gli Stati membri e tutti i portatori di interessi a collaborare per realizzare gli ambiziosi obiettivi del piano d'azione.

[52] ENISA, *EU Cybersecurity Index, Framework and Methodological Note* (2024). Disponibile all'indirizzo https://www.enisa.europa.eu/sites/default/files/2024-12/eu_csi_methodological_note_v1-0.pdf.

ALLEGATO - Sintesi delle azioni proposte

La Commissione:

Centro europeo di sostegno alla cibersicurezza per ospedali e prestatori di assistenza sanitaria dell'ENISA	
Garantire risorse adeguate per il centro di sostegno alla cibersicurezza Collaborare con l'ECCC per avviare progetti pilota volti a sviluppare migliori pratiche per l'igiene informatica e la valutazione dei rischi per la sicurezza e a far fronte alla necessità di monitorare la cibersicurezza in modo continuo, di disporre di un'intelligence sulle minacce e di rispondere agli incidenti utilizzando soluzioni di cibersicurezza all'avanguardia, per lo sviluppo del catalogo dei servizi del centro europeo di sostegno alla cibersicurezza	2025
Prevenzione degli incidenti di cibersicurezza	
In consultazione con gruppo di cooperazione NIS, EU-CyCLONe e ENISA, valutare la possibilità di considerare la sanità come un settore al quale può essere fornito sostegno per la verifica coordinata della preparazione a norma del regolamento sulla cibersolidarietà.	Primo trimestre 2025
Risposta e ripresa rapide	
Insieme all'ENISA, garantire che la riserva dell'UE per la cibersicurezza comprenda un servizio di risposta rapida destinato specificamente al settore sanitario	Quarto trimestre 2025
Cooperazione pubblico-privato	
Istituire, con il sostegno dell'ENISA, un comitato consultivo comune per la cibersicurezza del settore sanitario	Primo trimestre 2025
Pubblicare un invito ad agire destinato a imprese, fondazioni, istituti di istruzione e portatori di interessi del settore della cibersicurezza affinché si impegnino ad adottare misure per affrontare le sfide del settore sanitario	Secondo trimestre 2025
Scoraggiare gli autori delle minacce informatiche	

Valutare, insieme all'alto rappresentante, l'uso di misure del pacchetto di strumenti della diplomazia informatica per prevenire e scoraggiare le attività dolose contro i sistemi sanitari e rispondervi	2025
Promuovere la cooperazione internazionale contro gli autori di ransomware, in particolare nell'ambito dell'iniziativa internazionale Counter Ransomware, in collaborazione con l'alto rappresentante	2025-2026
Perseguire la cooperazione nell'ambito del gruppo di lavoro del G7 sulla cibersicurezza per rafforzare la cibersicurezza del settore sanitario	2025-2026
Prossime tappe	
Avviare ampie consultazioni dei portatori di interessi	Primo trimestre 2025
Adottare raccomandazioni per perfezionare ulteriormente il piano d'azione	Quarto trimestre 2025

L'ENISA:

Centro dell'UE di sostegno alla cibersicurezza per ospedali e prestatori di assistenza sanitaria	
Avviare i lavori per istituire un centro europeo di sostegno alla cibersicurezza per gli ospedali e i prestatori di assistenza sanitaria	Secondo trimestre 2025
Elaborare un catalogo completo dei servizi che dovranno essere forniti dal centro di sostegno alla cibersicurezza	A partire dal quarto trimestre 2025
Prevenzione degli incidenti di cibersicurezza	
Elaborare orientamenti che evidenzino le pratiche fondamentali in materia di cibersicurezza e assistere i prestatori di assistenza sanitaria nella loro attuazione	Terzo trimestre 2025
In stretta collaborazione con la Commissione e gli Stati membri, elaborare uno strumento di mappatura normativa	Primo trimestre 2025
Elaborare un quadro specifico per l'assistenza sanitaria per valutare la maturità della cibersicurezza	Terzo trimestre 2025
Effettuare una valutazione annuale della maturità della cibersicurezza in ambito sanitario	2025-2026

Collaborare con gli Stati membri e le autorità regionali responsabili dei programmi per creare programmi modello di voucher per la cibersicurezza	2025-2026
Elaborare nuovi orientamenti in materia di appalti per la cibersicurezza degli ospedali e dei prestatori di assistenza sanitaria	Terzo trimestre 2025
Creare una rete europea dei CISO del settore sanitario	Primo trimestre 2026
Progettare e promuovere moduli e corsi di cibersicurezza per gli operatori sanitari	Primo trimestre 2026
Capacità europee di rilevamento delle minacce informatiche dirette al settore sanitario	
Creare un catalogo europeo delle vulnerabilità note e sfruttate per i dispositivi medici, i sistemi di cartelle cliniche elettroniche e i fornitori di apparecchiature e software TIC in ambito sanitario	Quarto trimestre 2025
Introdurre un servizio di allarme rapido a livello dell'UE per il settore sanitario accessibile tramite iscrizione	Dal 2026
Sostenere l'ISAC europeo per il settore sanitario con strumenti e scambi di informazioni	2025-2026
Risposta e ripresa rapide	
Insieme alla Commissione, garantire che la riserva dell'UE per la cibersicurezza comprenda un servizio di risposta rapida destinato specificamente al settore sanitario	Quarto trimestre 2025
In collaborazione con la rete di CSIRT, sviluppare protocolli di risposta agli incidenti informatici specifici per l'assistenza sanitaria	Terzo trimestre 2025
Agevolare un'ampia diffusione delle esercitazioni nazionali di cibersicurezza per testare i protocolli e rafforzare la risposta agli incidenti	Dal quarto trimestre 2025
Fornire un servizio, accessibile tramite iscrizione, di ripresa da un attacco ransomware	Dal 2026
Insieme all'Europol, individuare i ceppi ransomware più comuni destinati alle organizzazioni sanitarie e ampliare l'archivio degli strumenti di decrittazione attraverso il progetto "No More Ransom"	Quarto trimestre 2025

Insieme a Europol, elaborare orientamenti accessibili per aiutare i prestatori di assistenza sanitaria a evitare il pagamento di riscatti	Terzo trimestre 2025
Azioni a livello nazionale	
Assistere gli Stati membri nell'elaborazione di piani d'azione nazionali	2025
Coordinare gli sforzi per garantire che le risorse e le strategie dei singoli Stati membri si completino a vicenda	2025-2026
Attuazione e monitoraggio del piano d'azione	
In consultazione con la Commissione, fornire alle reti pertinenti degli Stati membri regolari aggiornamenti sul lavoro del centro di sostegno alla cibersicurezza	2025-2026
Garantire scambi continui con il comitato consultivo per la cibersicurezza del settore sanitario	2025-2026

Gli Stati membri:

Capacità europee di rilevamento delle minacce informatiche dirette al settore sanitario	
Condividere con il centro europeo di sostegno alla cibersicurezza le notifiche di incidenti inviate da ospedali e prestatori di assistenza sanitaria a norma della direttiva NIS 2	Dal quarto trimestre 2025
Incoraggiare lo sviluppo di ISAC nazionali per il settore sanitario	2025-2026
Prevenzione degli incidenti di cibersicurezza	
Nell'ambito del gruppo di cooperazione NIS, effettuare una valutazione coordinata dei rischi per la sicurezza, valutando sia i rischi tecnici sia quelli strategici connessi alle catene di approvvigionamento dei dispositivi medici	Quarto trimestre 2025
Risposta e ripresa rapide	
Effettuare esercitazioni nazionali di cibersicurezza per testare i protocolli e rafforzare la risposta agli incidenti	Dal 2026
Azioni a livello nazionale	

Designare i centri nazionali di sostegno alla cibersicurezza per ospedali e prestatori di assistenza sanitaria	Secondo trimestre 2025
Elaborare piani d'azione nazionali incentrati sulla cibersicurezza nel settore sanitario	Quarto trimestre 2025
Facilitare la condivisione delle risorse tra i prestatori di assistenza sanitaria	2025-2026
Fissare parametri di riferimento non vincolanti e monitorare gli obiettivi di finanziamento specificamente destinati alla cibersicurezza	Quarto trimestre 2025
Chiedere alle organizzazioni sanitarie e ad altri soggetti interessati dalla direttiva NIS 2 di dichiarare la loro intenzione di pagare riscatti	Quarto trimestre 2025